The Premier Event for Search Engine Marketing & Optimization Search Engine Strategies 2005 December 5-8, 2005 • Chicago, IL

FREE Symantec Technical Whitepapers and Tools:

Whitepaper:	Whitepaper:	Whitepaper:	Whitepaper:
Symantec LiveState™ Client Management Suite	Symantec LiveState™ Delivery	Symantec LiveState™ Patch Manager	Symantec LiveState™ Recovery

Get Featured Whitepapers from the Novell Linux Solution Center

WHITEPAPER : Novell Support Solutions for Linux
Need a dynamic range of support solutions for Linux?

WHITEPAPER : Why Move from Windows NT to SUSE LINUX?
Migrate and take advantage of the reliability and security of Linux

WHITEPAPER : Why Choose Novell for Linux?
Why is Novell the best distribution vendor for Linux from both a technology and support standpoint?

WHITEPAPER : Ten Reasons to Choose SUSE LINUX over

Whitepaper: Using Radio Resource Management (RRM) to Deliver Secure and Reliable WLAN Services. Learn how RRM algorithms work and how real-time RF management can be used to improve WLAN operations.

EAP Developing Federated Authentication Policies

September 27, 2004
By Kevin Savetz

The struggle to remember two dozen different passwords to access two dozen Web sites could, one day, be a thing of the past. The days of requiring users to register for your Web site, then painstakingly verifying each user's identity, could similarly be passing.

Federated identity management will change the way consumers, businesses, and the government think about online authentication. That is, if the Electronic Authentication Partnership (EAP) does what it has set out to do.

The purpose of the stakeholder organization is to establish the rules that will let different authentication systems work together, not on a technological level, but on a policy level. The EAP is establishing technology-neutral procedures for federated identity management.

"A lot of people have focused on this as a technology problem. But there is a set of policy issues, of governance issues, that aren't being addressed. That's what the EAP is going to address," said Jim Lewis, interim chair of the EAP. Lewis is also senior fellow for the Center for Strategic and International Studies, a nonpartisan research organization.

Microsoft Windows.
Discover cost savings, speed and security.

internet.commerce
Be a Commerce Partner
Free PC Phone & IM
Memory Flash Cards
Managed Hosting
Dedicated Hosting
Compare Prices
Laptop Reviews
Search Engine Ranking
Music
Web Hosts
Cheap Plane Tickets
Add Video Ads
Mortgage Refinance
Search Web Hosting

The group is tackling issues such as assigning levels of trust for a credentialing system, determining rules for issuing credentials, and creating a process for accessing the trustworthiness of credentials. "Right now these are either ad hoc or nonexistent," Lewis said.

With these rules in place, disparate systems will be able to share authentication data and rely on the data provided by other systems. For instance, when a user wants to log into a bank or credit card Web site, an outside organization could, based on digital signature, guarantee that the user at the keyboard is indeed who he claims to be.

The 39 current members of the EAP include Wells Fargo Bank, VeriSign, Microsoft, and the U.S. General Services Administration (GSA) — a broad mix of service providers, credential issuers, trade groups, and governments.

Member organizations must agree to follow the EAP's rules regarding interoperability of electronic authentication systems. The EAP's rules, which are still being drafted, will have more teeth than a best-practices policy. A common problem with "best practices" groups is that they don't breed confidence, Lewis said. "'I promise that, on good days, I will try to –' that does not lead to trust. We need something that is a little tougher than best practices. We need people to commit to do these things, and to be accessed and tested," he said.

Related Articles

- IETF Shutters E-Mail Working Group
- VeriSign Unveils Two-Factor Authentication
- Netegrity Building on Its Access Management Base
- DomainKeys Set to Send Mail

XML/RSS feeds

XML RSS

EarthWeb IT Management news and headlines
Inside ID headlines
See more EarthWeb Network RSS feeds

FREE Tech Newsletters

Inside ID Weekly
your@email Sign Up

Members of the group hope to have a set of pilot rules in place by the end of the year, then formalize a final set in the second half of 2005.

The EAP's rules for interoperability of authentication systems will lower the costs and risk of online authentication for member organizations, Lewis said. "It lowers their costs because they may not have to get into the credentialing business — they may be able to use someone else's credentials. It lowers risk because when you get a credential you will have an external standard against which you can measure it."

One issue the group will have to tackle is how to determine the level of assurances that will exist for credentials. This will depend on the organization that issued the credential and how heartily it vouches for it.

Rules will follow models already established in the financial services sector. Under the EAP's plan, a credential may have any of four levels of assurance. More stringent vetting means a higher level of assurance, which would allow more sophisticated transactions. "You might need one level to go to a federal Web site and reserve space on a campground. You might need a different level if you want to check your social security file, and a different level to apply for a mortgage," said Helena Sims, secretariat of the EAP and senior director for public/private partnerships at NACHA, The Electronic Payments Association.

NACHA is providing staffing and behind-the-scenes support for the EAP while the fledgling group selects a board, files articles of incorporation, and manages other start-up tasks.

The federal government is a member of the organization. "We need common authentication services within the federal government. We didn't want 2,000 different ways to sign on to government Web sites," David Temoshok, vice chair of the EAP, said. Temoshok is the director

of identity policy and management for the GSA Office of Governmentwide Policy.

"We see federation of identity as necessary for what we need to do for providing common authentication services to the federal government," Temoshok said. It makes sense for industry to support the same or similar trust requirements, standards, and processes, he said. "There's a broader public interest here, as we create this big federation for the federal government, they ought to be able to do that outside of the federal government as well," he said.

Federated identity could ultimately make the Internet more useful and safer for everyone. After signing on to view an online statement at Wells Fargo, a user might be able to check an account at Charles Schwab, then be routed to the Social Security Administration to check on benefits and earnings, all without having to sign off from one system, sign on to another, and register at each.

"In order for us do to that in the federal government, we are going to have to trust that process by which the Wells Fargo customer signed on to their home banking account," Temoshok said.

A key will be doing so without relying on proprietary systems. "We are interested in being able to provide for multiple products, multiple technologies, multiple protocols, because the 280 million Americans out there are going to want to make choices," Temoshok said.

Kevin Savetz is a freelance technology writer who has written for more than 75 publications.

Enterprise ID Management Archives

Back to Home

White Paper: Information Management Trends In 2005

What's your current data focus? While some companies are still focused on storage and access, others are leveraging their information to be more agile, gain new insights into business performance and make better decisions. Get this white paper and learn how your peers are implementing their data management solutions. Download this whitepaper. Compliments of Sybase.

JupiterWeb networks:

internet.com | EARTHWEB | dev | graphics.com

Search JupiterWeb: Find

Jupitermedia Corporation has four divisions:
JupiterWeb, JupiterResearch, JupiterEvents and JupiterImages

Copyright 2005 Jupitermedia Corporation All Rights Reserved.
Legal Notices, Licensing, Reprints, & Permissions, Privacy Policy.

Jupitermedia Corporate Info | Newsletters | Tech Jobs | Shopping | E-mail Offers